Monitoring & Logging Guide: The PureIoT Visibility Strategy

Introduction

Effective monitoring and logging are essential for maintaining server health, diagnosing performance issues, and detecting security threats. This guide outlines the best practices for achieving full visibility into your server infrastructure.

1. Monitoring: Know Your Server's Health

Monitoring is about tracking the operational status and performance of your servers in real-time.

- **Key Metrics:** Monitor the "Golden Signals" of server health:
  - **Latency:** The time it takes to service a request.
  - **Traffic:** How busy the server is (e.g., network throughput, requests per second).
  - **Errors:** The rate of requests that fail.
  - **Saturation:** How full the server is (e.g., CPU utilization, memory usage).
- **Proactive Alerting:** Set up alerts for deviations from the established performance baseline (e.g., CPU usage above 90% for 5 minutes, disk space below 10%).
- **Synthetic Monitoring:** Use external tools to simulate user actions (e.g., logging into a web application) to test end-to-end service availability.

2. Logging: The Forensic Record

Logging provides the detailed, historical record needed for troubleshooting and security forensics.

- **Centralized Logging: Do not rely on local server logs.** Implement a centralized logging system (e.g., ELK Stack, Splunk, Graylog) to aggregate logs from all servers, applications, and network devices.
- **Structured Logging:** Logs should be in a structured format (e.g., JSON) rather than plain text. This makes them machine-readable and searchable.

- **Log Levels:** Use standard log levels correctly:
  - **DEBUG:** Detailed information, typically only used during development.
  - **INFO:** General operational messages.
  - **WARN:** An event that might indicate a problem.
  - **ERROR:** An event that prevents a requested operation from completing.
  - **CRITICAL:** A system-wide failure requiring immediate attention.
- **Security Information and Event Management (SIEM):** Use a SIEM system to analyze security logs in real-time, correlate events across multiple systems, and detect complex threats.

3. Best Practices for Implementation

- **Time Synchronization:** Ensure all servers and devices are synchronized to a central **NTP (Network Time Protocol)** server. Without synchronized time, log correlation for troubleshooting is impossible.
- **Log Retention:** Define a clear policy for how long logs are stored (e.g., 90 days for operational logs, 1 year for security/compliance logs).
- **Log Security:** Logs contain sensitive information. Ensure the centralized logging system is secured and access is restricted via the Principle of Least Privilege.

Monitoring & Logging Checklist

Item	Status	Notes
Centralized Logging System Deployed	[ ]	
Structured Logging Enabled	[ ]	
Proactive Alerts Configured	[ ]	For CPU, RAM, Disk, Errors
All Servers Time-Synchronized (NTP)	[ ]	
Security Logs Feeding into SIEM	[ ]	

Conclusion

Visibility is security. By implementing a robust monitoring and centralized logging strategy, you can move from reactive firefighting to proactive, preventative maintenance. PureIoT provides fully managed monitoring and SIEM services for complete infrastructure visibility.